

UNITED STATES DISTRICT COURT

for the
District of Oregon

FILED 14 JAN 19 1157 USDC-ORP

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
 11875 SW Center Street, Apartment 82
 Beaverton, OR 97005
)
)
)
) Case No.
)
)
)

'19 -MC- 21

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

11875 SW Center Street, Apartment 82 Beaverton, OR 97005, as described in Attachment A

located in the _____ District of Oregon , there is now concealed (*identify the person or describe the property to be seized*):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 2, 371, 1952,
2421

Offense Description
Conspiracy to use a facility in interstate commerce with intent to promote acts to facilitate the promotion and carrying of a business enterprise involving prostitution and transporting an individual in interstate commerce for purposes of prostitution.

The application is based on these facts:

See affidavit of FBI Special Agent June Piniewski which is attached hereto and incorporated hereinby this reference.

Continued on the attached sheet.

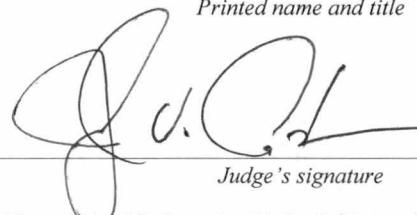
Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

June Piniewski, FBI Special Agent

Printed name and title



Judge's signature

Hon. John V. Acosta, United States Magistrate Judge

Printed name and title

Sworn to before me and signed in my presence.

Date: 01/12/2019

City and state: Portland, Oregon

DISTRICT OF OREGON, ss:

AFFIDAVIT OF JUNE PINIEWSKI

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, June Piniewski, being duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation (FBI), and have been so employed since February 2015. As a Special Agent of the FBI, I am authorized to investigate violations of the criminal laws set forth in Title 18 of the United States Code. I am currently assigned to the Portland Division of the FBI where I investigate violations of federal law, including bank robberies, crimes against children, sex trafficking offenses, and other violent crimes. I have been involved in multiple investigations of matters involving sex trafficking, particularly as it relates to violations of 18 U.S.C. §§ 1591, 1952, 2421, and 2423. I have had extensive training in law enforcement investigation techniques, including but not limited to 800 hours of training at the FBIs Academy at Quantico, Virginia. Prior to joining the FBI, I was a Deputy Sheriff in Hillsborough County, Florida, for approximately five years.

2. As a Special Agent of the FBI, I am authorized to investigate violations of the criminal laws set forth in Title 18 of the United States Code. I am currently assigned to the Portland Division of the FBI where I investigate violations of federal law, including bank robberies, crimes against children, sex trafficking offenses, and other violent crimes. I have been involved in multiple investigations of matters involving sex trafficking, particularly as it relates to violations of 18 U.S.C. § 2421.

3. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following premises: **11875 SW**

Center Street, Apartment 82, Beaverton, OR (Location 1), for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section §§ 2, 371, 1952, and 2421. As set forth below, I have probable cause to believe that such property and items, as set forth in Attachment B, which is attached hereto and incorporated herein by this reference, including any digital devices or electronic storage media, are currently on the premises located above, more fully described in Attachment A, which is also attached hereto and incorporated herein by this reference.

4. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the search warrant application, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2, 371, 1952, and 2421, exists on the person of **Chenglan Huang**, and at the apartment, located at: ***11875 SW Center Street, Apartment 82, Beaverton, OR (Location 1.)***

Applicable Law

6. Title 18, United States Code, Section 1952(a)(3) makes it a crime to knowingly use a facility in interstate or foreign commerce, specifically computers and cellular telephones, with intent to promote, manage, establish, and carry on acts to facilitate the promotion,

management, establishment, and carrying on of an unlawful activity namely, a business enterprise involving prostitution offenses in violation of the laws of the State in which they are committed, to-wit prostitution in violation of Oregon Revised Statute (ORS) 167.007 and of the United States, and thereafter performed and attempted to perform an act to promote, manage, establish, and carry on and to facilitate the promotion, management, establishment, and carrying on of such unlawful activity; Title 18, United States Code, Section 2421 makes it a federal felony for anyone to knowingly transport an individual in interstate or foreign commerce, with the intent that such individual engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so. Title 18, United States Code, Section 371, makes it a crime for two or more persons to conspire to commit any offense against the United States and for one or more of the people to do any act to effect the object of the conspiracy. Title 18, United States Code, Section 2 provides that whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission is punishable as a principal.

STATEMENT OF PROBABLE CAUSE

Sex Trafficking

7. I have received formal and on-the-job training in the investigation of sex trafficking. I have participated in several investigations, which led to the arrest and conviction of traffickers, and have become familiar with the habits, mannerisms, language, and techniques used in committing human trafficking offenses, and the attempts to conceal the evidence of such occurrences from detection by both the public at large and law enforcement agencies. I have spoken with and read documentation by officers who possess knowledge and expertise in the investigation of sex trafficking-related crimes. I have spoken to numerous victims of sex

trafficking about their experiences in the life of prostitution. I have also participated in many aspects of sex trafficking investigations, including conducting physical surveillance, interviews, reviewing electronic evidence, using confidential human sources, writing and executing search and seizure warrants, and making arrests. I have gained knowledge of the inner working of Sex Trafficking Organizations (STOs) and based on my training and experience know the following:

8. Prostitution is inherently a cash business, as cash provides paying customers with some form of anonymity. STOs often move and launder the cash by placing it into bank accounts, using casinos to launder sources of cash, wire transfers, store value credit/debit cards, online e-currency, investment accounts, real estate, cash-based businesses such as restaurants, and other types of assets. STOs will often move the illegal proceeds several times through different forms of assets to make it difficult for law enforcement to discover the true source of the funds. STOs will often open legitimate businesses or have legitimate employment to launder the illegal proceeds and comingle these illegal funds with legitimate income from the business or employment, to prevent law enforcement from discovering the true source of the proceeds.

9. Websites such as, www.backpage.com, www.adultsearch.com, www.supermatchescort.com, www.portlandasianescort.com and others are often used by STOs to advertise commercial sex services.¹ I know that STOs will often advertise their services as “massages” or “escorts” to avoid detection by law enforcement. The term “escort” is widely used as a euphemism for prostitution. I know that a legitimate “escort” is hired for an extended period of time such as several hours and even days. An “escort” is expected to be attractive and presentable in public. They are often used to stand-in as a date for specific functions or

¹ On April 6, 2018, Backpage.com was shutdown and seized by the government due to allegations it was promoting sex trafficking and prostitution. Since this occurred, we have observed that people who used to post on Backpage.com have now started using other sites.

entertainment for an evening. "Escorts" are paid for their time and their company and sexual favors are not included as part of their package. Legitimate "escorts" or "massage" parlors do not list coded language for the services they provide such as: GFE (Girlfriend Experience) or BBJ (Bare Blowjob). I also know that legitimate "escorts" or "massage" parlors do not typically advertise services posting sexually provocative photographs or by providing age, height or the weight of the person providing the massage. Legitimate "escort" and "massage" businesses typically do not operate from a motel room paid on a day-by-day basis, nor from an apartment. I also know legitimate "escorts" and "masseuses" do not perform sexual acts on their customers and therefore do not provide condoms or wear lingerie when interacting with the customer.

10. The STOs post on-line ads for "escorts" or "massages" that investigators recognize as prostitution-related advertisements. The investigation has revealed the following roles within a STO:

- a. *Customers* – men who pay money for sexual acts
- b. *Providers* – individuals who perform sex acts for money
- c. *Drivers* – individuals who transport the providers and perform other activities, such as: collecting proceeds, delivering food and other supplies
- d. *Leasee* – individuals who lease the apartments that are used as brothels
- e. *Dispatcher* – individuals who answer the calls/texts/emails (responses to ads) from the customers and sets up "dates" within the computer and notifies the provider
- f. *Boss* – a supervisor of one or more brothel locations

11. Through this investigation, I have learned how STOs manage operations of the online ads. When a customer responds to the ad and calls the number associated with the ad,

they are connected to “dispatch.” Dispatch identifies the location of the customer and assigns the customer to a specific provider (someone who performs sex acts for money) for a “date” (an encounter for the purposes of engaging in a commercial sex act with the women). Dispatch then notifies the provider that a “date” has been set.

12. STOs arrange apartments and hotels for the provider to stay in and use for engaging in acts of prostitution. As part of the investigation, law enforcement has conducted over twenty undercover sting operations in Portland, Oregon, targeting Asian “escort” ads. In these sting operations, an undercover officer sets up a “date” using the contact phone number provided in the ad. After confirming the date and obtaining an address through the STO dispatch, the undercover officer is told to notify dispatch when they have arrived. Once the undercover has arrived, dispatch will provide the motel room number or apartment number.

13. Once inside the apartment, investigators notice very little furniture and that the bedroom in the apartment appears to be only used for sex acts. Investigators rarely see a bedframe and often the mattress has just a sheet with a towel laid on top. The nightstands next to the bed usually have multiple unused condoms on or near them, towels, and various bottles of oils and lubricants. The clothing in the closets or in the suitcases consist of mainly of lingerie.

14. The STOs recruit women to work as providers from their respective countries (generally China or other Asian countries) and the women generally speak very little English. Some providers have indicated they are engaging in prostitution to pay back certain costs, such as the cost of coming to the United States.

15. For the past two years, I have been investigating sex trafficking, mainly focused on Asian STOs. As the investigation unfolded, I learned multiple agencies (both local and federal) across the country have encountered Asian STOs. The investigation revealed multiple

Asian STOs operating throughout the United States. As part of the investigation we have also come across several smaller STOs which appear to be operating independently within the Greater Portland Metro area. These STOs are also using various on-line advertisements to solicit customers for the purposes of engaging in prostitution.

Location 1 – 11875 SW Center Street, Apartment 82, Beaverton, OR

16. According to a report written by Task Force Officer (TFO) Chad Opitz, on August 24, 2017, based upon information he had received he conducted surveillance at 11975 SW Center Street, Beaverton, OR (Willow Grove apartment complex). He determined that multiple females were more likely than not advertising and offering prostitution services from an apartment within the complex. Beaverton Police Detective Sergeant Mark Groshong told TFO Opitz that he had located ads on www.backpage.com in the "women seeking men" section that he believed were prostitution related, where the females advertised they were in Beaverton on SW Center Street. Sergeant Groshong text one of the phone numbers in an undercover capacity and received a text message saying they were at 11975 SW Center Street, but did not give an individual unit number.

17. TFO Opitz, went on Backpage.com and found multiple ads related to SW Center Street. The two primary phone numbers for the ads were "503-994-9188" and "503-837-8989." One of the ads was titled "Hot Independent ASIAN GIRL," "100% Real," and listed the number 503-994-9188. The ad, which included multiple pictures of scantily clad Asian appearing women, read:

SWEET BEAUTY NO NEED TO LOOK ANY FURTHER! ONE OF BP'S FINEST ASIAN! Gorgeous & Friendly Korean with an hourglass figure & a Great Rack! Outgoing, Friendly, Funny, & Sweet BEST OF THE BEST! 100% TRULY MIND BLOWING EXPERIENCE! . . . WILL EXCEED ALL YOUR EXPECTATIONS B2B NURU * SHOWER * GF

* TOUCH * KISS * 69 & MORE Call Text: 503-994-9188
BEAVERTON Portland

18. TFO Opitz, and myself, both recognize this to be a prostitution related advertisement. The references to "B2B" and "NURU" is a body-to-body and skin to skin massage; "GF" is a reference to a girlfriend experience, which is prostitution related acts that include kissing; and, "69" is a reference to a sexual position. All of these references are ones that we have seen in many prostitution related advertisements.

19. While doing the surveillance, TFO Opitz saw numerous males drive into the complex and go into apartment #1 of the 11975 building. The males would generally be at the apartment between 15 and 30 minutes.

20. On August 31, 2017, while acting in an undercover capacity, TFO Opitz sent a text message to 503-994-9188 inquiring about a "date." He immediately got a reply saying that they were available and that it was "160/30min" and "200/hr." TFO Opitz agreed to an hour date around 12:00 p.m. The following is a summary of the conversation:

TFO Opitz: Hi gorgeous can I come see you at noon today?
503-994-9188: yes come here? 160/30min and 200/1hr
TFO Opitz: where is here? Hr is good!
503-994-9188: willow grove 11975 sw center st OR 97005
503-994-9188: get address?
TFO Opitz: Yup!
503-994-9188: see u then^^
TFO Opitz: On what apt?
503-994-9188: give u room when here lol
TFO Opitz: Oh ok
TFO Opitz: Still good for noon?
503-994-9188 yes hon
TFO Opitz: Thx!
TFO Opitz: 12 good still?
503-994-9188: yes baby
TFO Opitz: Just pulled in
TFO Opitz: Where do I go?
503-994-9188: turn left when drive in, 11975 around the corner by trash dumpster, parking any spot without shed

TFO Opitz: I am Here and Horny?

503-994-9188: sorry to ask r u black gentleman baby?

TFO Opitz: Nope!

503-994-9188: unit 1 no knock thx

21. When we arrived at the apartment complex, TFO Opitz sent a text message to 503-994-9188 advising that he had arrived. He was told to come to unit #1 of 11975 SW Center Street but not to knock. From his training and experience, TFO Opitz knows this is common for the females to ask for customers not to knock so that less attention is brought to the place and neighbors aren't alerted to people constantly coming over.

22. As TFO Opitz approached the front door to apartment #1, it was opened and he observed an Asian female inside. The Asian female invited TFO Opitz inside the apartment, he stopped at the doorway to the apartment and verbally identified himself as a police detective. He also showed the female his law enforcement detective badge. He observed that the female was wearing lingerie/sleepwear. He could see that the female was holding a pink colored cell phone. He removed the cell phone from the female's hands placed it on the clothes dryer, which was just inside the door. The female was walked outside the apartment and an announcement to see if there was anyone else inside the residence was made. From the kitchen/living room area of the residence, another Asian female subject came out and she also walked from the apartment. The apartment was checked for additional people and no one else was located inside.

23. A FBI linguist was on scene and provided translation between law enforcement and the two Asian females, who turned out to be Chinese. The female that originally came to the door was identified as Shuang Zhao. The other female found inside the apartment was identified with an International Driver's License as Chenglan Huang.

24. Using the FBI linguist as an interpreter, Huang and Zhao both gave consent for law enforcement to search the interior of the apartment. The apartment was a two bedroom unit and each bedroom contained a mattress set. There was no furniture in the living room of the apartment. In the living room, were rolls of paper towels and bathroom tissue that were stacked up. In the kitchen area, were cases of water bottles that were stacked up. This is consistent to what TFO Opitz had seen when doing surveillance. He had seen that when the suspected "johns" left the apartment they were each carrying water bottles. The following other items were located inside the apartment: Kirkland Brand products; a large plastic bag found in the outside storage closet that contained a significant amount of Kimono Special brand condoms; a plastic, rectangular shaped gum container that contained 24 unused, but unwrapped condoms (this gum container was found on the kitchen counter; additional packaged condoms were also found in the kitchen in a cabinet under the counter; US currency was found in the kitchen, however it was not a significant amount (under \$100) and left at the scene; a Bank of America deposit slip showing that \$800 was deposited earlier in the day was found on the dining room table; a Costco card belonging to Zhongping Zhang was found in a silver colored suitcase in one of the bedrooms; a piece of paper found in a kitchen drawer that had the address 1100 N. Anchor Way handwritten on it; and four (4) cell phones.

25. On August 31, 2017, Shuang Zhao was interviewed. I explained that the interview would be recorded and she was not under arrest and free to leave at any time and was not obligated to provide a statement, Zhao agreed to answer the questions asked of her. The following is a summary of the interview:

She came to the United States approximately two years ago on September 15, 2015. She flew from China to San Francisco and then to New York. The purpose of her coming to the U.S. was to be a tourist. She eventually found a boyfriend

and that is why she stayed. She paid for her own travel over to the U.S. and doesn't owe anyone money. She currently lives in Flushing, New York but doesn't know her address. She worked in New York sometimes at a restaurant as a dishwasher or waitress. She also worked at a massage place in Brooklyn, NY and gives massages. The boss known as "CoCo", helps her arrange her customers. The massage place is called 16 Ave Spa, located at 7209 16th Avenue Brooklyn, NY. She learned about the job at the 16 Ave Spa through an advertisement in the newspaper. The newspaper can be purchased anywhere and costs \$.50. "CoCo" comes to the business about once or twice a week. Each massage is for one hour and costs the customer \$50. She is paid \$10 plus tips for each massage. She stated she was here in Portland to work and "CoCo" does not know she is here. The female inside the apartment (later identified as Chenglan Huang) told Zhao to come to Portland from New York to work. She has only talked to her via WeChat. She contacted her daughter back in China to buy her a ticket from New York to Portland. She sends money back to her daughter who lives with her parents. She flew American Airlines flight 87 to get to Portland and arrived in Portland on August 29, 2017.

When Zhao arrived, Huang told her to give her her passport and she would give it to her "friend" because it is safer. She does not know who the boss is in Portland. She found out about the "business" out here while in a WeChat group. She just arrived in Portland a couple of days ago. When she arrived at the Portland airport an "UBER" was called for her and took her to the apartment. Since she arrived at the apartment she has given three massages so far and has earned a little over \$100. She kept some of the money and Huang told her to give her the rest. Zhao was asked by investigators if she ever performed any "sexual acts" and she stated she only gave massages.

26. On August 31, 2017, Chenglan Huang was interviewed. I explained that the interview would be recorded and she was not under arrest and free to leave at any time and was not obligated to provide a statement, Huang agreed to answer the questions asked of her.

27. The following is a summary of the interview:

Huang has been in the United States since the beginning of January 2017. She stated flew from China to Los Angeles and then to Seattle for a bit until she came to Portland. Huang advised that she was "robbed" in Seattle and had no documents on her to identify her. An International Driver's License was found for Huang in the apartment and she stated it was hers. Huang was asked about the "business" and how long she had been working. She replied that she doesn't know much, she has never met anyone, you go online and "they" give you an address to go somewhere to work and when you're done they will give you another address to work. Huang stated she just got to the current address yesterday (August 30, 2017) and does not know the other girl that was inside the

apartment with her. It cost her \$35 to get from Seattle to Portland and the driving service took her straight to the apartment. She stated that she does not know anything about how the "business" works. She just opens the door when a customer shows up and does whatever the customer says. There was a driver that comes to pick up the money from time to time but she never paid attention to what he looked like. The people who come to pick up the money separates some for her and she just takes whatever they give her. Huang also stated the "drivers" are always "American" men.

28. From late 2017, until around June 2018, ongoing video surveillance was conducted on the Willow Grove Apartment complex, Apartment # 1, located at 11975 SW Center Street, Beaverton, Oregon. The video surveillance regularly showed males going into and out of the apartment, often up to nine different men in a day, and staying only for relatively short periods of time. By way of example, attached is Video 1, which is time edited surveillance video showing men coming and going from the location throughout the day and night of February 25, 2018.

29. On December 21, 2018, Task Force Officer (TFO) Chad Opitz located a female Asian escort ad. The ad was titled, "SUPER JUICE SEXYYOUNGASIAN GIRL 200% REAL" and contained the contact number "503-917-0083." The advertisement, which included multiple pictures of a scantily clad Asian appearing woman, read:

NO YOUNG NO PAY I am sweet and well trained and know how to pamper you. Hey, I am a HOT & SUPER SEXY YOUNG ASIAN Girl Everything U Need is Right Here! – FULL BODY RUB AND MORE FUN!! – HOT Body to Body Busty& petite lovely SENUAL TOUCH + NUDE Bodyslide DUO SHOWER TOGETHER,OIL NURU MASSAGE, 360 ROTATION, KISSING, CALL : 503-917-0083

TFO Opitz and I recognize this to be a prostitution related advertisement, specifically the references to the physical attributes of the woman and "360 rotation," "kissing," "shower together," and "more fun," which are indicative of prostitution related activities. TFO Opitz texted the number and had the following conversation:

TFO Opitz: Wherein Beaverton you located? Looking for a duo. Hr date
503-917-0083: 11875 SW Center St Beaverton, OR 97005 Willow Grove APT
(On the right side) \$200/hour, \$160/half hour Cash only No black guy. Thanks
TFO Opitz: 200 for both girls? Or is that more? I am white
503-917-0083: One
TFO Opitz: Can I have a date with 2 girl?
503-917-0083: Yes
503-917-0083: 400
TFO Opitz: Ok thx. I will let you know
TFO Opitz: How soon can I come over to see you 2 girls?
503-917-0083: Anytime
TFO Opitz: Ok. Will come at 10. Is that apartments? What unit do I go to?
503-917-0083: Apt, get here I send u
TFO Opitz: Ok
TFO Opitz: Ok just pulling into lot. What one at 11875 do I go to?
503-917-0083: Are u here?
TFO Opitz: Yes. Just trying to figure out where to go
503-917-0083: How long u want stay?
TFO Opitz: 1 hr...
TFO Opitz: This is weird you aren't telling me where to go. Kinda nervous
503-917-0083: Give me few moniutes honey
TFO Opitz: Do I leave?
503-917-0083: Waiting please honey
TFO Opitz: I can see just one if easier
503-917-0083: Ready now
503-917-0083: Still here?
TFO Opitz: But where do I go?
TFO Opitz: What number?
503-917-0083: Room 82
TFO Opitz: Room 82? Isn't this an apartment
503-917-0083: Yes
503-917-0083: Apt
503-917-0083: Coming?
TFO Opitz: A cop just drove thru the lot. Something isn't right. This is a set up?
503-917-0083: Don't worry
503-917-0083: Safe
503-917-0083: Come or not?

30. On December 21, 2018, I contacted the property manager from the Willow Grove Apartments and learned the following: approximately two weeks ago four people came into the leasing office to rent Apartment 82, Bin Zhang, Chee Yai Hui, Chenglan Huang, and John Patrick Thompson. All four people filled out rental applications. The property manager was told

that both Zhang and Hui had to go back to China so they would not be renting. It was also advised to property management that Huang needed a translator because she did not speak English. On Zhang's and Hui's applications they provided a previous address of: 590 NW Lost Springs Terrace, Portland OR 97229. This Lost Springs Terrace address has come up in other undercover prostitution operations conducted in mid 2018, like those described above, where an undercover officer has responded to an on-line advertisement and been directed to go to this address.

31. On December 27, 2018, I served a Grand Jury subpoena to the property manager at the leasing office of the Willow Grove Apartments for all the information related to the residents at 11875 SW Center St, Apartment 82, Beaverton, OR. The leasing office is located directly across from building 11875 SW Center St Apt 82. While in the office, I observed a silver GMC truck bearing Oregon tag 937CAB in front of building 11875. A search of law enforcement databases provided that the truck was registered to Weijun Chen. In the bed of the truck was a box spring wrapped in plastic. I observed an Asian male and an Asian female exit the bottom area of the building. The unidentified male and female removed the mattress and brought it into apartment 82. They then came back and grabbed a box (unknown items inside) and cases of water and brought them into the apartment.

32. Also while inside the leasing office, a man later identified as Thompson came in to pay the rent for apartment 82. He used a Wells Fargo check (#2669) and in the memo section wrote, "Jan rent #82." He exited the building and entered the driver's side of a Lexus bearing Oregon tag 158JYP and left the complex. A search of law enforcement databases provided that the vehicle was registered to Thompson.

33. While inside the leasing office, the property manager then advised that maintenance needed to enter apartment 82 due to an oven issue. I entered the apartment with the maintenance crew and the property manager. While inside the two bedroom apartment I observed the following: an Asian female, minimal furniture, two mattresses and box springs in the living room area, one mattress and box spring on the floor of each bedroom, used condoms and tissues within the garbage can of the bathroom, cases of water, and a suit case in the closet of one of the bedrooms.

34. On January 11, 2019, I talked to the property manager for the Willow Grove Apartments at 11875 SW Center St, Beaverton, OR. The property manager told me that Apartment 82 is still being leased by the same people and that they have consistently seen multiple men coming and going from Apartment 82 throughout the day.

Knowledge of STOs and Request for Items to Seize²

35. As described above and in Attachment B, this application seeks permission to search for various physical items, including records (in whatever form they are found) that may be found on the Premises identified above that I know are evidence, instrumentalities, and fruits,

² Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address.* The Internet Protocol address (or simply “IP address”) is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

of violations of Title 18, United States Code, Sections 2, 371, 1952, and 2421, involving individuals engaged in criminal conspiracy to knowingly transport individuals in interstate and foreign commerce with intent that such individuals engage in prostitution and who are using a facility in interstate commerce with the intent to promote, manage, establish, carry on and facilitate the promotion, management, establishment, and carrying on of unlawful prostitution activities.

36. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

37. Through my training and experience and involvement in this investigation, I have learned that prostitution is primarily, and its base level involving a date between a provider and a customer, a cash based business. When money is collected by a provider it then starts to get transferred to other people, including to a boss, as well as others within the organization, in a variety of forms. Once the money is received, it is also often converted or used to buy both physical items of value as well as property. Finding currency and currency equivalents representing the proceeds of illegal activities, money wrappers, and other documents and items evidencing the obtaining, expenditure, transfer, and/or concealment of assets are evidence of the underlying criminal activity. Documents relating to real estate transactions including but not limited to: loan and mortgage records, correspondence with financial institutions, customer or nominee information, documents relating to closings and real estate transactions, documents reflecting monies paid or received, lease agreements, customer account information, income and

expenses summaries, cash disbursement journals, financial statements, state and federal income tax returns help provide evidence of the underlying criminal activity. Bank records including but not limited to: receipts, bank and savings and loan records of deposit, statements, and other bank records, letters of credit, money orders, cashier's checks, passbooks, canceled checks, certificates of deposit, and other documents reflecting financial transactions help provide evidence of the underlying criminal activity. Other financial records including but not limited to: cash disbursement journals, financial statements, states of account, deposit slips, money orders, cashier's checks, and related receipts, canceled checks, check registers, passbooks, credit card records and receipts, any records related to digital money transfers, letters of credit, ledgers, tax returns, and any other records pertaining to the receipt, expenditure, or concealment of income also help provide evidence of the underlying criminal activity. I also know that individuals will often hide these items, including within safes.

38. Through my training and experience and involvement in this investigation, I have learned that providers and the STOs involved in prostitution regularly keep records, both in terms of scheduling "dates," but also documenting information about their customers, information about the providers, contact lists, items purchased, others involved in the organization, and the money made, owed, and transferred.

39. Through my training and experience and involvement in this investigation, I have learned that the providers involved in prostitution regularly use and supply condoms, lotions, and other sexual paraphernalia to service clients.

40. Through my training and experience and involvement in this investigation, I have learned that many of the providers involved in the STO under investigation are from Asian countries. I have also learned that in these types of investigations that the providers, and other

people involved in the criminal activity, do not always provide their true names and thus U.S. or foreign identification documents, U.S. or foreign passports, birth certificates and records, driver's licenses, identification cards, employment identification, immigration documents, naturalization certificates, etc. which may be used to establish identity, citizenship, eligibility, residence, or domicile are important items of evidence to prove the identity of the involved individuals.

41. Through my training and experience and involvement in this investigation, I have learned that the STO is regularly moving and helping to facilitate the transportation of various providers both internationally and throughout the United States. I thus seek permission to search and seize any travel records including but not limited to payment or confirmation for: airline tickets, bus/train tickets, hotel/motel receipts, Uber, Lyft, taxi, and airport purchases that is evidence of this activity which has been done to advance the criminal activity under investigation.

42. Through my training and experience and involvement in this investigation, I have learned that individuals involved in the STO under investigation extensively use cellular phones to communicate through voice, text, and photo messages, which are often coded to conceal their true meaning from others, to carry out and facilitate their illegal activities.

43. Through my training and experience and involvement in this investigation, I have learned that the STO maintains electronic records of prostitution activity and/or advertising via computer or handheld electronic device and/or electronic data storage medium and thus seek to search for and seize any electronic devices, phones, computers, and tablets.

44. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know that the STO

under investigation heavily uses computers, cellular telephones, and other electronic devices to schedule prostitution “dates,” to communicate with customers, and to communicate with others in the organization.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Based on actual inspection of other evidence related to this investigation, including email search warrants, I am aware that digital devices were used to generate, store, and print documents used to promote the illegal prostitution activities that we are investigating. Thus, there is reason to believe that there is a digital device currently located on the Premises listed above that we seek to search. From my experience, every provider that we have encountered has at least had a cellular telephone.

45. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a digital device to commit the crimes under investigation the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

46. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to

analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

47. Based upon my training and experience, it is likely that the Premises will contain at least one Apple brand device, such as an iPhone or iPad, because we have encountered iPhones during this investigation.

a. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

b. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

c. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These

circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

d. The passcode or password that would unlock the Apple device found during the search of the Premises is not known to law enforcement. Thus, it will likely be necessary to press the fingers of the users of the Apple device found during the search of the Premises to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the users is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

e. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the

device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the Premises to press their fingers against the Touch ID sensor of the locked Apple device found during the search of the Premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

f. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the Premises as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

g. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of the above-named individuals found at the Premises to the Touch ID sensor of the device(s), such as an iPhone or an iPad, found at the Premises for the purpose of attempting to unlock the device(s) via Touch ID in order to search the contents as authorized by this warrant.)

48. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

49. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

50. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

51. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

52. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

53. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to

questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

54. Based on the foregoing, I have probable cause to believe that Chenglan Huang and other known and unknown individuals are engaged in knowingly transporting individuals in interstate and foreign commerce with intent that such individuals engage in prostitution and are knowingly using a facility in interstate or foreign commerce, specifically computers and cellular telephones, with intent to promote, manage, establish, and carry on acts to facilitate the promotion, management, establishment, and carrying on of an unlawful activity namely, a business enterprise involving prostitution offenses in violation of the laws of the State in which they are committed, to-wit prostitution in violation of Oregon Revised Statute (ORS) 167.007 and of the United States, and thereafter performed and attempted to perform an act to promote, manage, establish, and carry on and to facilitate the promotion, management, establishment, and carrying on of such unlawful activity and I do believe, that the premises described in Attachment A contains evidence contraband, and instrumentalities of violations of 18 U.S.C. §§ 2, 371, 1952 and 2421, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the premises described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

///

///

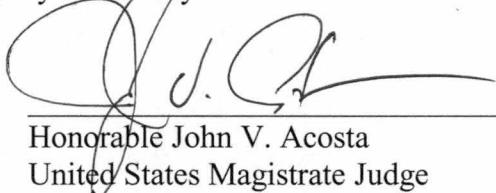
///

55. This affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney Scott Kerin prior to being submitted to the Court. AUSA Kerin informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



June Piniewski
Special Agent, FBI

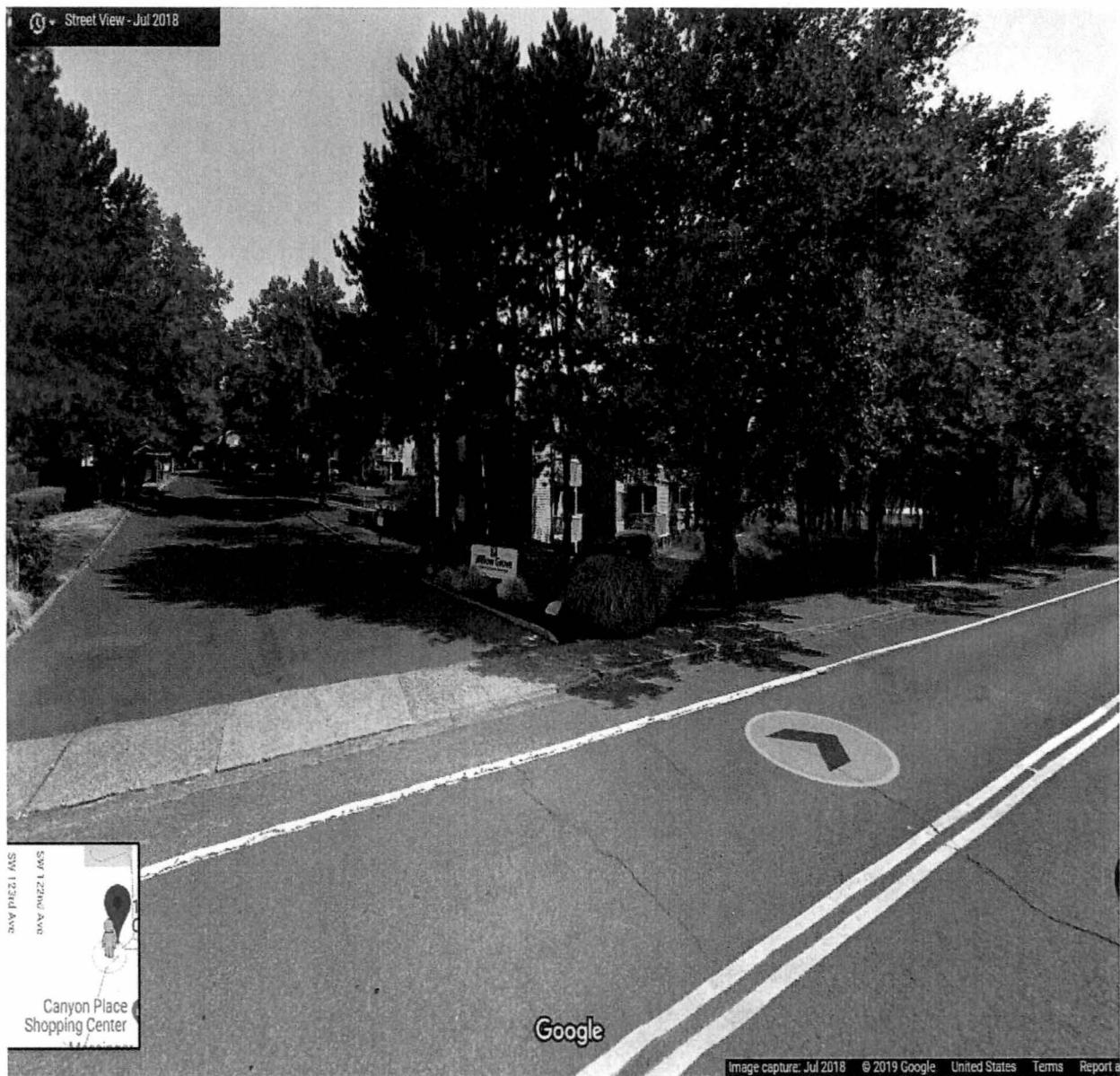
Subscribed and sworn to before me this 14th day of January 2019.



Honorable John V. Acosta
United States Magistrate Judge

ATTACHMENT A

11875 SW Center Street, Apartment 82, Beaverton, OR 97005 is a two bedroom apartment within the Willow Grove Apartment complex. The apartment is on the lower level, tan in color, with the number “82” on the door.



ATTACHMENT A



Attachment B**Items to be Seized**

The items to be searched for, seized, and examined, are those items on the premises located at the premises, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2, 371, 1952, and 2421, involving individuals engaged in criminal conspiracy to knowingly use a facility in interstate or foreign commerce, specifically computers and cellular telephones, with intent to promote, manage, establish, and carry on acts to facilitate the promotion, management, establishment, and carrying on of an unlawful activity namely, a business enterprise involving prostitution offenses in violation of the laws of the State in which they are committed, to-wit prostitution in violation of Oregon Revised Statute (ORS) 167.007 and of the United States, and thereafter performed and attempted to perform an act to promote, manage, establish, and carry on and to facilitate the promotion, management, establishment, and carrying on of such unlawful activity and who are knowingly transporting individuals in interstate and foreign commerce with intent that such individuals engage in prostitution and who are using a facility in interstate commerce with the intent to promote, manage, establish, carry on and facilitate the promotion, management, establishment, and carrying on of unlawful prostitution activities. The items to be seized cover the period of January 2017, through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:

a. Currency and currency equivalents representing the proceeds of illegal activities, money wrappers, and other documents and items evidencing the obtaining, expenditure, transfer, and/or concealment of assets;

- b. Tickets, logs, notes or items used to represent the number of clients served and money owed to a female being prostituted.
- c. Any condoms, lotions, or other paraphernalia used to service clients;
- d. U.S. or foreign identification documents, U.S. or foreign passports, birth certificates and records, driver's licenses, identification cards, employment identification, immigration documents, naturalization certificates, etc. which may be used to establish identity, citizenship, eligibility, residence, or domicile;
- e. Documents relating to correspondence with financial institutions, customer or nominee information, documents relating to closings and real estate transactions, documents reflecting monies paid or received, lease agreements, customer account information, income and expenses summaries, cash disbursement journals, financial statements, state and federal income tax returns;
- f. Bank records including: receipts, bank and savings and loan records of deposit, statements, and other bank records, letters of credit, money orders, cashier's checks, passbooks, canceled checks, certificates of deposit, and other documents reflecting financial transactions;
- g. Other financial records including: cash disbursement journals, financial statements, states of account, deposit slips, money orders, cashier's checks, and related receipts, canceled checks, check registers, passbooks, credit card records and receipts, any records related to digital money transfers, letters of credit, ledgers, tax returns, and any other records pertaining to the receipt, expenditure, or concealment of income;
- h. Fruits of crimes and items of value that evidence wealth obtained from the sex trafficking, including: United States currency, precious metals, jewelry, safe deposit

box lease agreements and safe deposit box keys, and other items of value, as well as books and records regarding the acquisition, use, and disposition of such items of value;

- i. Safes and the contents of any safes, locked or unlocked;
- j. Any travel records including but not limited to payment or confirmation

for: airline tickets, bus/train tickets, hotel/motel receipts, Uber, Lyft, taxi, and airport purchases.

k. Cellular telephones, computers and other electronic devices capable of storing data that constitutes evidence or the instrumentality of the crimes identified above.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

- a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.
- b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
- c. Evidence of the lack of such malicious software.
- d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.
- e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.
- f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.
- h. Evidence of the times the Computer was used.
- i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.
- j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

4. During the execution of the search of the Premises described in Attachment A, law enforcement personnel are authorized to press the fingers, including thumbs, of (name the individuals) found at the Premises to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the Premises for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

Search Procedure

5. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

6. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the

warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

9. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

10. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential

exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

19-MC-211

Video

|

